

**IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK**

-----x
JAMES ROBINSON, individually and on : Case No.: 1:14-cv-04146-RA
behalf of all others similarly situated, :
: Plaintiff, :
: v. :
: DISNEY ONLINE d/b/a DISNEY INTERACTIVE, :
a California Corporation, :
: Defendant. :
-----x

**FIRST AMENDED CLASS ACTION COMPLAINT
AND DEMAND FOR JURY TRIAL**

Plaintiff James Robinson (“Robinson”) brings this First Amended Class Action Complaint and Demand for Jury Trial (“Complaint”) against Defendant Disney Online d/b/a Disney Interactive (“Disney”) to put an end to its unlawful practice of disclosing its users’ sensitive information, and to obtain redress for such conduct. Plaintiff, for his Complaint, alleges as follows upon personal knowledge as to himself and his own acts and experiences and, as to all other matters, upon information and belief, including investigation conducted by his attorneys:

NATURE OF THE ACTION

1. The Walt Disney Company is one of the largest entertainment-media companies in the world. Perhaps best known for its eponymous amusement parks and resorts, Disney is also an international publisher of news and entertainment media. The Walt Disney Company, through

its subsidiary Defendant Disney Online,¹ offers its news and entertainment programming to consumers via a variety of mediums, including through its proprietary software application (the “Disney Channel”) that it developed for use with a digital media-streaming device called the Roku.²

2. Unbeknownst to its users, each time they use the Disney Channel to watch videos or television shows, Disney discloses their personally identifiable information—including a record of every video clip viewed by the user (collectively, “PII”—to unrelated third parties. In addition to demonstrating a brazen disregard for its users’ privacy rights, Disney’s actions also violate the Video Privacy Protection Act, 18 U.S.C. § 2710 (“VPPA” or the “Act”), which prohibits companies from disclosing their customers’ video viewing records to third parties without express written consent.

3. Disney’s violations of the VPPA are particularly flagrant here, as it programmed the Disney Channel to transmit users’ PII to a third-party data analytics company. The business models of such “big data” analytics companies center on the collection of disparate pieces of uniquely identifying information and online behavioral data about individual consumers, which they then compile to form comprehensive profiles about a person’s entire digital life. These profiles can then be used for targeted advertising, sold as a commodity to other data brokers, or both.

4. In an era when the collection and monetization of consumer data proliferates on an unprecedented scale, it’s important that companies are held accountable for the exploitation of

¹ About Disney Interactive, <http://www.disneyinteractive.com/about/> (last visited August 21, 2014).

² Roku is a digital media-streaming device that delivers videos, news, games, and other content to consumers’ televisions via the Internet.

their users' sensitive information. Disney chose to disregard Plaintiff's and thousands of other users' statutorily protected privacy rights by releasing their sensitive data into the marketplace. Accordingly, Plaintiff brings this Complaint against Disney for its intentional and unlawful disclosure of his PII in violation of the VPPA.

PARTIES

5. Plaintiff James Robinson is a natural person and citizen of the State of New York.

6. Defendant Disney Online is a corporation existing under the laws of the State of California with its principal place of business located at 500 South Buena Vista Street, Burbank, California 91521. Disney conducts business throughout this District, the State of New York, and the United States.

JURISDICTION AND VENUE

7. This Court has jurisdiction over the subject matter of this action pursuant to 28 U.S.C. § 1331 as this action arises under the VPPA. This Court has personal jurisdiction over Defendant because it conducts business in this District, The Walt Disney Company maintains an office and is registered to conduct business in this District, and the unlawful conduct alleged in the Complaint occurred in, was directed to, and/or emanated from this District.

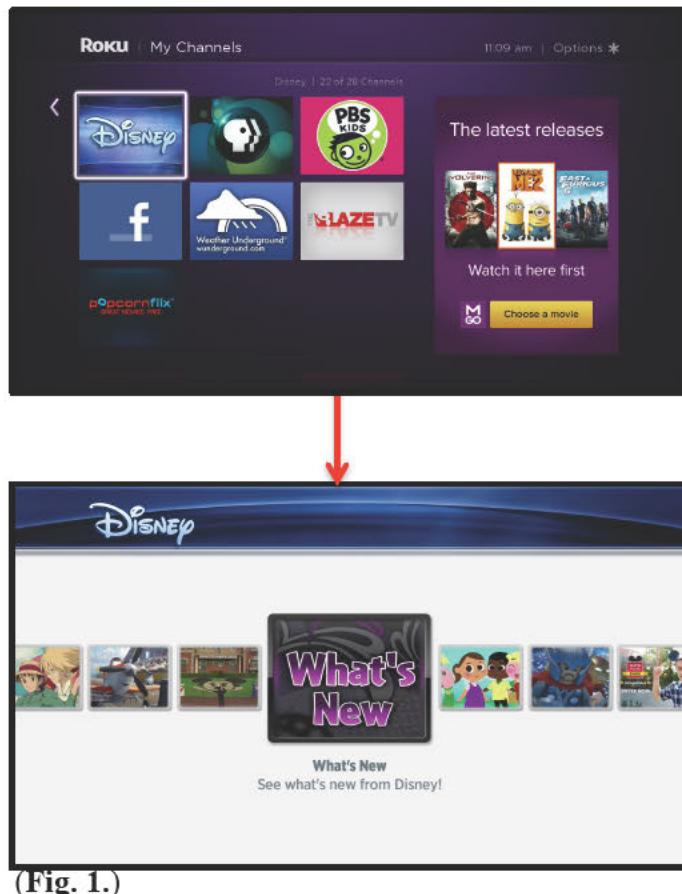
8. Venue is proper in this District under 28 U.S.C. § 1391(b) because Defendant conducts business in this District, The Walt Disney Company maintains an office and is registered to conduct business in this District, and the improper conduct alleged in this Complaint occurred in, was directed to, and/or emanated from this District. Venue is additionally proper because Plaintiff resides in the State of New York.

FACTUAL BACKGROUND

I. Disney Programmed the Disney Channel to Transmit Its Users' PII and Video Viewing Activity to a Third-Party Data Analytics Company Without Their Consent.

9. The Disney Channel is a digital software application that allows consumers to view Disney programming on their televisions via the Roku media-streaming device.

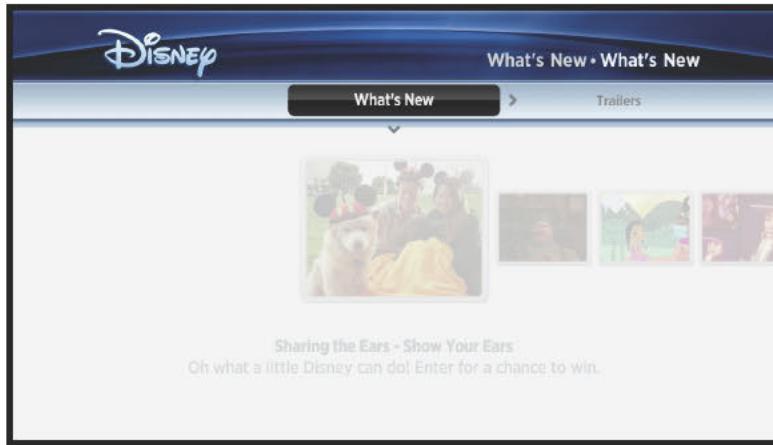
10. To install the application on a Roku, users must visit the Roku Channel Store—Roku's proprietary online digital media platform where users can download applications (called “channels”) that allow them to view specific television shows or video clips on their devices. Once downloaded and installed, and upon opening the application, the Disney Channel presents a main home screen that allows the user to view certain of Disney's proprietary video content. (See Figure 1, showing the Disney Channel's main home screen.)



11. At no time during this process, however, does Disney seek or obtain the consent of the user to share or otherwise disclose his or her PII to third parties for any purpose.

1. *The Disney Channel sends its users' video viewing activity and uniquely identifying PII to the third-party data analytics company Adobe.*

12. The Disney Channel is organized into categories accessible through the software's main user interface. (*See Figure 1* on the previous page; *see also Figure 2* below, showing the Disney Channel's graphical user interface.) Users may browse around these sections to do things like view video clips of television shows from Disney's cable channel. (*See id.*)



(Fig. 2.)

13. Unbeknownst to its users, however, each time they view a video clip, the Disney Channel sends a record of such activities to unrelated third-party data analytics company, Adobe.³ The complete record is sent each time that a user views a video clip, along with the hashed⁴ serial number associated with the user's Roku device.

³ Adobe is a company that offers data analytics and online marketing services that it claims "allow [its] customers to create groundbreaking digital content, deploy it across media and devices, measure and optimize it over time, and achieve greater business success." *See* Adobe Company, <http://www.adobe.com/company.html?promoid=JZPLK> (last visited May 23, 2014). Using its services, Adobe says, helps companies "make, manage, measure, and monetize their content across every channel and screen." *Id.*

⁴ "Hashing" refers to a process whereby data is converted into a fixed-length, shortened

14. The data transmitted from a Roku device while a user watches video clips on the Disney Channel facially appear to be sent to the domain “go.com”, which is owned by Disney. However, technical examination reveals that the actual servers receiving the information are maintained by Adobe.

15. The effect of this design is two-fold: first, it creates the outward appearance that Adobe isn’t collecting any user information—personally identifiable or otherwise—through the use of the Disney Channel. Second, it permits Adobe to circumvent security measures the Roku device may implement to prevent Adobe from storing and collecting information from users watching the Disney Channel.⁵ These practices are particularly troubling given Adobe’s reach in the analytics industry, as described in Section II below.

II. Data Analytics Companies Rely on Unique Identifiers Associated with Digital Devices to Create Dossiers On Consumers and Their Digital Behaviors.

16. Today’s average consumer uses more than one device to access the Internet to do things like view digital content or make online purchases. This creates challenges for online advertisers and data analytics companies. Namely, to gain a broad understanding of a given consumer’s behavior across all of the devices and applications that he or she uses, these companies have to find ways to “link” their digital personas. The primary solution has been to use certain unique identifiers to connect the dots.

17. To do this, data analytics companies—like Adobe—rely in part on creating user identities from information supplied by device manufacturers.

format that acts as a reference point to the original input data.

⁵ Implementing First-Party Cookies,
http://microsite.omniture.com/t2/help/en_US/whitepapers/first_party_cookies/ (last visited August 21, 2014).

18. An example of a device-manufacturer-supplied-user identity in the consumer electronics context is a device’s serial number. That’s because device serial numbers are “persistent identifiers,” meaning they are unique to a specific device and remain constant for the lifetime of the user’s device. Device serial numbers operate as persistent identifiers even when hashed, because each unique serial number has a corresponding unique hashed value.⁶ Thus, each hashed value will be unique to a specific device and remain constant for the lifetime of that device.

19. Roku itself explicitly acknowledges that its devices’ serial numbers are linked to the identities of their purchasers. In its Privacy Policy, Roku states that “[u]sage information uploaded from Roku Devices is personally identifiable by product serial number” and that the identifier can even be used to determine, among other demographic information, the precise store and location where the product was purchased.⁷

20. Once a Roku serial number (whether hashed or in plain-text)⁸ is matched with an individual’s identity, it’s exceedingly difficult for that person to avoid being tracked via their device—making it among the most stable and reliable identifiers for a given individual.

21. For these reasons, developers of software for the Roku rely on the device’s serial number to identify and track individual users.⁹

⁶ See Ashkan Soltani, *Federal Trade Commission Mobile Device Tracking Spring Privacy Series* at 14, Federal Trade Commission (Feb. 19, 2014), available at http://www.ftc.gov/system/files/documents/videos/spring-privacy-series-mobile-device-tracking/ftc_spring_privacy_series_-_mobile_device_tracking_-_transcript.pdf.

⁷ Roku Privacy Policy, <http://www.roku.com/about/privacy> (last visited June 4, 2014).

⁸ Because hashed serial numbers (like their plain-text counterparts) are unique, they are as useful as plain-text serial numbers in acting as unique identifiers.

⁹ See Parker Higgins and Lee Tien, *Mobile Tracking Code of Conduct Falls Short of Protecting Consumers*, Electronic Frontier Foundation (Oct. 26, 2013),

1. *Adobe and other data analytics companies maintain massive digital dossiers on consumers.*

22. Once a consumer's identity is matched with their device's serial number (or other "persistent identifier"), a wealth of extremely precise information can be gleaned about the individual. For instance, software applications that transmit a Roku's serial number along with the user's activity provide an intimate look into how the user interacts with their channels, which can reveal information such as the user's political or religious affiliation, employment information, articles and videos viewed, and even detail about the sequence of events in which the user interacts with their Roku.

23. An excerpt from Adobe's marketing materials, shown in Figure 3 below, accurately portrays the frightening array of information that feeds into a consumer's digital dossier using data transmitted from sources such as their digital devices.

Types of Customer Data	Characteristics	Source
One-to-One Data		Single Marketing View of Customer
Scoring Attributes	Lifetime value, RFM, risk score,	Customer Data Warehouse/Business Analytics
Implicit Customer Data (Behavioral Information)	Navigation history, opens, clicks, online transactions, other (POS, loyalty card activity...)	Web Analytics, Email, Mobile
Explicit Customer Data	Areas of interest, favorite products...	Form Capture, Landing Pages, Website
Computed Data	Estimated age, type of home...	Customer Data Warehouse/Business Analytics
Sociodemographic Data	Age, category, household structure, income	CRM, Third-Party Data Augmentation
Contact Information	Name, first name, address, email, phone number (home, business, or cell)	CRM

(Fig. 3.)

24. Figure 3 provides insight into the depth of information captured and stored by Adobe's data analytics services. Of particular note are the "sources" of consumer data in the far right column. The graphic's references to these sources—including "Web Analytics" and "Customer Data Warehouse[s]"—implicate software applications (like Disney's for the Roku) that collect consumer data. From such sources, Adobe is able to amass the wealth of information on the left in Figure 3. That information includes things like: a person's name, address, age, phone number, email, purchase history, behavioral activity, and income.

25. Indeed, marketing materials hosted on Adobe's website discuss at length how analytics companies (like Adobe) use disparate pieces of information collected about consumers to identify and track their behavior.¹⁰ For instance, a report published on Adobe's website states that "[p]eople leave many markers when they interact with a company, including a record of the web pages they visited and the purchases they made . . . Factors such as time of day, geographical location, device, and browser indicate a user's current situation. Organizations can map this data to aggregate information about similar users to help predict what an individual may be trying to achieve at a given point in time."¹¹

26. The Privacy Policy for Adobe's analytics services also states that: "[s]ome companies using Adobe services may send us information that allows them to identify you personally. Some companies may also buy additional information about you and then add that additional information to the information collected by Adobe's products on their websites. This

¹⁰ Test, Target, Personalize, and Profit, <http://www.adobe.com/solutions/testing-targeting.html> (last visited August 21, 2014).

¹¹ See Anjali Yakkundi and Ron Rogowski, *Advance To Next-Generation Personalization* at 3, Forrester Research, Inc. (Jan. 13, 2014), available at [http://offers.adobe.com/content/dam/offer-manager/en/na/marketing/Target/Advance_To_Next_Generatio%20\(1\).pdf](http://offers.adobe.com/content/dam/offer-manager/en/na/marketing/Target/Advance_To_Next_Generatio%20(1).pdf).

additional information may include things like email addresses, account information, or Facebook profile information, including photos and usernames.”¹²

27. In other words, Adobe’s materials describe how it may combine information in its databases from various sources to form a comprehensive profile about a consumer. One of those sources is assuredly Roku; because it associates users’ identities with their Roku’s serial number, Adobe needs only to link existing personal information (whether it obtains the data from Roku or elsewhere) with a Roku device to discover the person’s identity and their video records.

28. And Roku admits to sharing information about its users’ as well. In its Privacy Policy, Roku asserts that, “Roku may also share information with companies integral to the use of our products. For example, we may share information collected from the Roku Devices with content providers which have developed channels for the Roku Channel Store. The use of data by those content providers is subject to their respective privacy policies.”¹³

29. Accordingly, in this context Adobe has the capability to use data obtained from both the Disney Channel and Roku—and or additional sources—to personally identify its users and associate their video viewing selections with a personalized profile in its databases.

2. *The President and Congress are responding to growing privacy concerns over the collection and misuse of personal information in the digital marketplace.*

30. Concerns over the privacy risks associated with the collection and transmission of PII from digital devices to third parties is no longer just academic musing. In a recently issued sixty-two page policy memo, President Obama squarely addressed the issue, stating that there’s a growing problem with consumers’ privacy “in the age of the Internet, the World Wide Web and

¹² Analytics and on-site personalization services, <http://www.adobe.com/content/dotcom/en/privacy/analytics.html> (last visited June 4, 2014).

¹³ Roku Privacy Policy, <http://www.roku.com/about/privacy> (last visited June 4, 2014).

smartphones.”¹⁴ While the President’s memo provided a “blueprint” for protecting consumers’ privacy, he called on Congress to take the lead and pass legislation to curb behavior related to the corporate exploitation of user data.

31. For its part, Congress has started to take up these issues as well. In 2011, Senators Patrick Leahy and Al Franken established the United States Senate Committee on the Judiciary, Subcommittee on Privacy, Technology, and the Law that, among other things, oversees the laws and policies governing (i) the collection, protection, use and dissemination of commercial information by the private sector, including online behavioral advertising, privacy within social networking websites and other online privacy issues, (ii) privacy standards for the collection, retention, use and dissemination of personally identifiable commercial information, and (iii) privacy implications of new or emerging technologies.¹⁵

32. In establishing this Subcommittee, Senator and Subcommittee Chair Al Franken noted that “[t]he boom of new technologies over the last several years has made it easier to keep in touch with family, organize a community and start a business . . . It has also put an unprecedented amount of personal information into the hands of large companies that are unknown and unaccountable to the American people.”¹⁶

33. Members of other subcommittees have made similar remarks. In a meeting of the Subcommittee on Consumer Protection, Product Safety, and Insurance, Senator John Rockefeller

¹⁴ Consumer Data Privacy In a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy, <http://www.whitehouse.gov/sites/default/files/privacy-final.pdf> (last visited June 4, 2014).

¹⁵ United States Senate Committee on the Judiciary, Subcommittee on Privacy, Technology and the Law, <http://www.judiciary.senate.gov/about/subcommittees/privacytechnology.cfm> (last visited Mar. 5, 2014).

¹⁶ Sen. Franken To Chair New Subcommittee on Privacy, Technology and the Law, http://www.franken.senate.gov/?p=hot_topic&id=1315 (last visited June 4, 2014).

noted that, “third parties use [consumer data] to target advertising on individuals . . . It is very good business, but it is very cynical. It is an abuse of that power, passing on people’s profiles.”¹⁷

34. In response to the increased scrutiny on consumers’ privacy concerns, companies are also starting to change their data collection and usage practices. For instance, in the release of Apple’s most recent mobile device operating system, iOS 7, it discontinued the ability to transmit certain personally identifiable information to third parties for tracking purposes.¹⁸

35. Despite the controversy surrounding these methods of harvesting and commodifying sensitive consumer data, Disney chose to disclose Disney Channel users’ sensitive information to the third-party data analytics company Adobe.

III. The VPPA’s Importance in the Digital Age.

36. When the VPPA was introduced, the late Senator Paul Simon noted that, “[e]very day Americans are forced to provide to businesses and others personal information without having any control over where that information goes. These records are a window into our loves, likes, and dislikes.” S. Rep. No. 100-599 at 7–8 (1988). Senator Patrick Leahy, one of the original drafters of the VPPA, also remarked that, “the trail of information generated by every transaction that is now recorded and stored in sophisticated record-keeping systems is a new, more subtle and pervasive form of surveillance.” *Id.* at 8.

37. While these statements rang true in 1988 when the act was passed, the need for legislation like the VPPA in the modern computing era is more pronounced than ever before.

¹⁷ S. Hrg. 112-289, Consumer Privacy and Protection in the Mobile Marketplace, <http://www.gpo.gov/fdsys/pkg/CHRG-112shrg73133/html/CHRG-112shrg73133.htm> (last visited June 4, 2014).

¹⁸ iOS 7 Eliminates MAC Address as Tracking Option, Signaling Final Push Towards Apple’s Own Ad Identifier Technology, <http://techcrunch.com/2013/06/14/ios-7-eliminates-mac-address-as-tracking-option-signaling-final-push-towards-apples-own-ad-identifier-technology/> (last visited May 23, 2014).

During a recent Senate Judiciary Committee meeting, “The Video Privacy Protection Act: Protecting Viewer Privacy in the 21st Century,” Senator Leahy emphasized this point, saying that, “[w]hile it is true that technology has changed over the years, we must stay faithful to our fundamental right to privacy and freedom. Today, social networking, video streaming, the ‘cloud,’ mobile apps and other new technologies have revolutionized the availability of Americans’ information.”¹⁹

38. Likewise, Senator Al Franken summed up the importance of the VPPA in today’s world as follows: “[i]f someone wants to share what they watch, I want them to be able to do so . . . But I want to make sure that consumers have the right to easily control who finds out what they watch—and who doesn’t. The Video Privacy Protection Act guarantees them that right.”²⁰

IV. Plaintiff Robinson’s Experience with the Disney Channel.

39. Starting in December 2013, Plaintiff Robinson downloaded and began using the Disney Channel on his Roku media-streaming device to watch certain Disney video clips.

40. At all times relevant, Robinson did not consent, agree, or otherwise permit Disney to disclose his PII to any third-party data analytics companies.

41. Likewise, Robinson has never been given the opportunity to prevent the Disney Channel from disclosing his PII to third parties.

42. Nevertheless, each time Robinson viewed a video clip using the Disney Channel, Disney disclosed his PII—including the first 15 characters of the titles of the videos he watched, along with a hashed version of his Roku device’s unique serial number, which is used by Roku

¹⁹ Patrick Leahy, *Statement of Senator Patrick Leahy At A Hearing On The Video Privacy Protection Act*, leahy.senate.gov (Jan. 31, 2012), <https://www.leahy.senate.gov/press/statement-of-senator-patrick-leahy-at-a-hearing-on-the-video-privacy-protection-act>.

²⁰ *Chairman Franken Holds Hearing on Updated Video Privacy Law for 21st Century*, franken.senate.gov (Jan. 31, 2012), https://www.franken.senate.gov/?p=hot_topic&id=1923.

and others to identify him—to the third-party data analytics company Adobe.

CLASS ALLEGATIONS

43. **Class Definition:** Plaintiff brings this action pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3) on behalf of himself and a Class of similarly situated individuals, defined as follows:

All persons in the United States who used the Disney Channel to watch videos and who had their PII transmitted to Adobe.

Excluded from the Class are (1) Defendant, Defendant's agents, subsidiaries, parents, successors, predecessors, and any entity in which Defendant or its parents have a controlling interest, and those entity's current and former employees, officers, and directors, (2) the Judge to whom this case is assigned and the Judge's immediate family, (3) persons who execute and file a timely request for exclusion from the Class, (4) persons who have had their claims in this matter finally adjudicated and/or otherwise released, and (5) the legal representatives, successors, and assigns of any such excluded person.

44. **Numerosity:** The exact number of members of the Class is unknown and is not available to Plaintiff at this time, but individual joinder in this case is impracticable. The Class likely consists of thousands of individuals. Class members can be easily identified through Defendant's records.

45. **Commonality and Predominance:** There are many questions of law and fact common to the claims of Plaintiff and the other members of the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include but are not limited to the following:

- a) Whether Defendant, through the Disney Channel, unlawfully disclosed and continues to unlawfully disclose its users' personally identifiable information, including their video viewing records, in violation of

18 U.S.C. § 2710(b);

- b) Whether Defendant's disclosures were committed knowingly;
- c) Whether Defendant disclosed Plaintiff's and Class members' personally identifiable information without their consent; and
- d) Whether Defendant violated Plaintiff's and Class members' rights to privacy.

46. **Typicality:** Plaintiff's claims are typical of the claims of the other members of the Class. Plaintiff and the Class sustained damages as a result of Defendant's uniform wrongful conduct during transactions with Plaintiff and the Class.

47. **Adequate Representation:** Plaintiff will fairly and adequately represent and protect the interests of the Class, and has retained counsel competent and experienced in complex litigation and class actions. Plaintiff has no interests antagonistic to those of the Class, and Defendant has no defenses unique to Plaintiff. Plaintiff and his counsel are committed to vigorously prosecuting this action on behalf of the members of the Class, and have the financial resources to do so. Neither Plaintiff nor his counsel has any interest adverse to those of the other members of the Class.

48. **Policies Generally Applicable to the Class:** This class action is appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class as a whole, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the members of the Class, and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply and affect members of the Class uniformly and Plaintiff's challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to

Plaintiff. Defendant has acted and failed to act on grounds generally applicable to Plaintiff and the other members of the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward members of the Class. The factual and legal bases of Defendant's liability to Plaintiff and to the other members of the Class are the same, resulting in injury to the Plaintiff and to all of the other members of the Class. Plaintiff and the members of the Class have suffered harm and damages as a result of Defendant's unlawful and wrongful conduct.

49. **Superiority:** This case is also appropriate for certification because class proceedings are superior to all other available methods for the fair and efficient adjudication of this controversy. The injuries suffered by the individual members of the Class are likely to have been relatively small compared to the burden and expense of individual prosecution of the litigation necessitated by Defendant's actions. Absent a class action, it would be difficult, if not impossible, for the individual members of the Class to obtain effective relief from Defendant. Even if members of the Class themselves could sustain such individual litigation, it would not be preferable to a class action because individual litigation would increase the delay and expense to all parties and the Court and require duplicative consideration of the legal and factual issues presented herein. By contrast, a class action presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single Court. Economies of time, effort, and expense will be fostered, and uniformity of decisions will be ensured.

50. Plaintiff reserves the right to revise the foregoing "Class Allegations" and "Class Definition" based on facts learned through additional investigation and in discovery.

FIRST CAUSE OF ACTION
Violations of 18 U.S.C. § 2710
(On behalf of Plaintiff and the Class)

51. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

52. Defendant is a “video tape service provider[]” as defined by the VPPA because it “engage[s] in the business, in or affecting interstate or foreign commerce, of rental, sale, or delivery or prerecorded video cassette tapes or similar audio visual materials,” 18 U.S.C. § 2710(a)(4), because it provides video (*i.e.*, “similar audio visual materials” under the VPPA’s definition) to consumers via its Disney Channel.

53. Plaintiff is a “consumer” as defined by the VPPA because he downloaded and installed the Disney Channel on his Roku device, and subsequently watched videos through the Disney Channel. 18 U.S.C. § 2710(a)(1). Under the Act, this means that he was a “subscriber” of “goods or services from a video tape service provider.” *See id.* Additionally, because Defendant grants him a temporary license to access and view specific videos in exchange for him being exposed to Defendant’s advertisements, Plaintiff is also a “renter” of video content from Defendant.

54. Under the VPPA, the term “personally identifiable information” “includes information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider.” 18 U.S.C. § 2710(a)(3). The definition’s usage of the word “includes” means that a more expansive reading of the term was expressly contemplated.

55. While the Disney Channel was installed on his Roku, Plaintiff viewed numerous video clips using the channel. On information and belief, during these occasions the Disney Channel disclosed the serial number of Plaintiff’s Roku and records of the videos he viewed to

the third party analytics company Adobe.

56. As detailed more fully in Section II.1 above, the information disclosed by the Disney Channel—the combination of the hashed Roku serial number and video viewing records—constitutes “personally identifiable information” in this context because it allows Adobe to identify users (such as Plaintiff), and to attribute their video viewing records to their existing profiles.

57. Thus, Defendant’s disclosure of Plaintiff’s hashed Roku serial number and video viewing records allowed Adobe to use its existing databases to identify him and attribute his viewing choices to his profile.

58. Consistent with this view, the National Institute of Standards and Technology (NIST) defines “personally identifiable information” as “any information that can be used to distinguish or trace an individual’s identity.”²¹ As discussed in Section II and throughout this Complaint, Plaintiff’s hashed Roku serial number and video viewing records can be used by Adobe to distinguish or trace his identity.

59. Defendant’s transmissions of Plaintiff’s PII to Adobe constitute “knowing[] disclosures” of Plaintiff’s “personally identifiable information” to a person as proscribed by the VPPA. 18 U.S.C. § 2710(a)(1).

60. At no time did Plaintiff ever provide Disney with any form of consent—either written or otherwise—to disclose his PII to third-parties.

61. Nor were Disney’s disclosures made in the “ordinary course of business” as the term is defined by the VPPA. In particular, the Disney Channel’s disclosures to Adobe were not

²¹ NIST Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), <http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf> (last visited Feb. 17, 2014).

necessary for “debt collection activities, order fulfillment, request processing, [or] the transfer of ownership.” 18 U.S.C. § 2710(a)(2).

62. As a result of Defendant’s unlawful disclosures, Plaintiff and the Class have had their statutorily defined right to privacy violated. Plaintiff seeks an injunction prohibiting Defendant from releasing his and the Class’s PII in the future, as well as the maximum statutory and punitive damages available under the VPPA. 18 U.S.C. § 2710(c).

PRAYER FOR RELIEF

WHEREFORE, Plaintiff James Robinson, on behalf of himself and the Class, respectfully requests that this Court enter an order:

- A. Certifying this case as a class action on behalf of the Class defined above, appointing Plaintiff James Robinson as representative of the Class, and appointing his counsel as Class Counsel;
- B. Declaring that Defendant’s actions, as set out above, violate the VPPA, 18 U.S.C. § 2710;
- C. Awarding injunctive and other equitable relief as necessary to protect the interests of the Class, including, *inter alia*, an order prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;
- D. Awarding damages, including statutory damages of \$2,500 per violation, and punitive damages, where applicable, in an amount to be determined at trial pursuant to 18 U.S.C. § 2710(c);
- E. Awarding Plaintiff and the Class their reasonable litigation expenses and attorneys’ fees;
- F. Awarding Plaintiff and the Class pre- and post-judgment interest, to the extent

allowable; and

G. Awarding such other and further relief as equity and justice may require.

JURY TRIAL

Plaintiff demands a trial by jury for all issues so triable.

Respectfully submitted,

JAMES ROBINSON, individually and on behalf
of all others similarly situated,

Dated: August 22, 2014

By: /s/ Benjamin H. Richman
One of Plaintiff's Attorneys

Fred B. Weinstein
fweinstein@kelaw.com
KURZMAN EISENBERG CORBIN & LEVER, LLP
1 North Broadway
White Plains, New York 10601
Tel: 914.993.6057
Fax: 914.993.6025

Rafey S. Balabanian (Admitted *Pro Hac Vice*)
rbalabanian@edelson.com
Benjamin H. Richman (Admitted *Pro Hac Vice*)
brichman@edelson.com
J. Dominick Larry (Admitted *Pro Hac Vice*)
nlarry@edelson.com
EDELSON PC
350 North LaSalle Street, Suite 1300
Chicago, Illinois 60654
Tel: 312.589.6370
Fax: 312.589.6378

CERTIFICATE OF SERVICE

I, Benjamin H. Richman, an attorney, hereby certify that on August 22, 2014, I served the above and foregoing ***First Amended Class Action Complaint and Demand for Jury Trial***, by causing a true and accurate copy of such paper to be filed and served on all counsel of record via the Court's CM/ECF electronic filing system, on this 22nd day of August 2014.

/s/ Benjamin H. Richman